

Fig. 2

FIG. 3

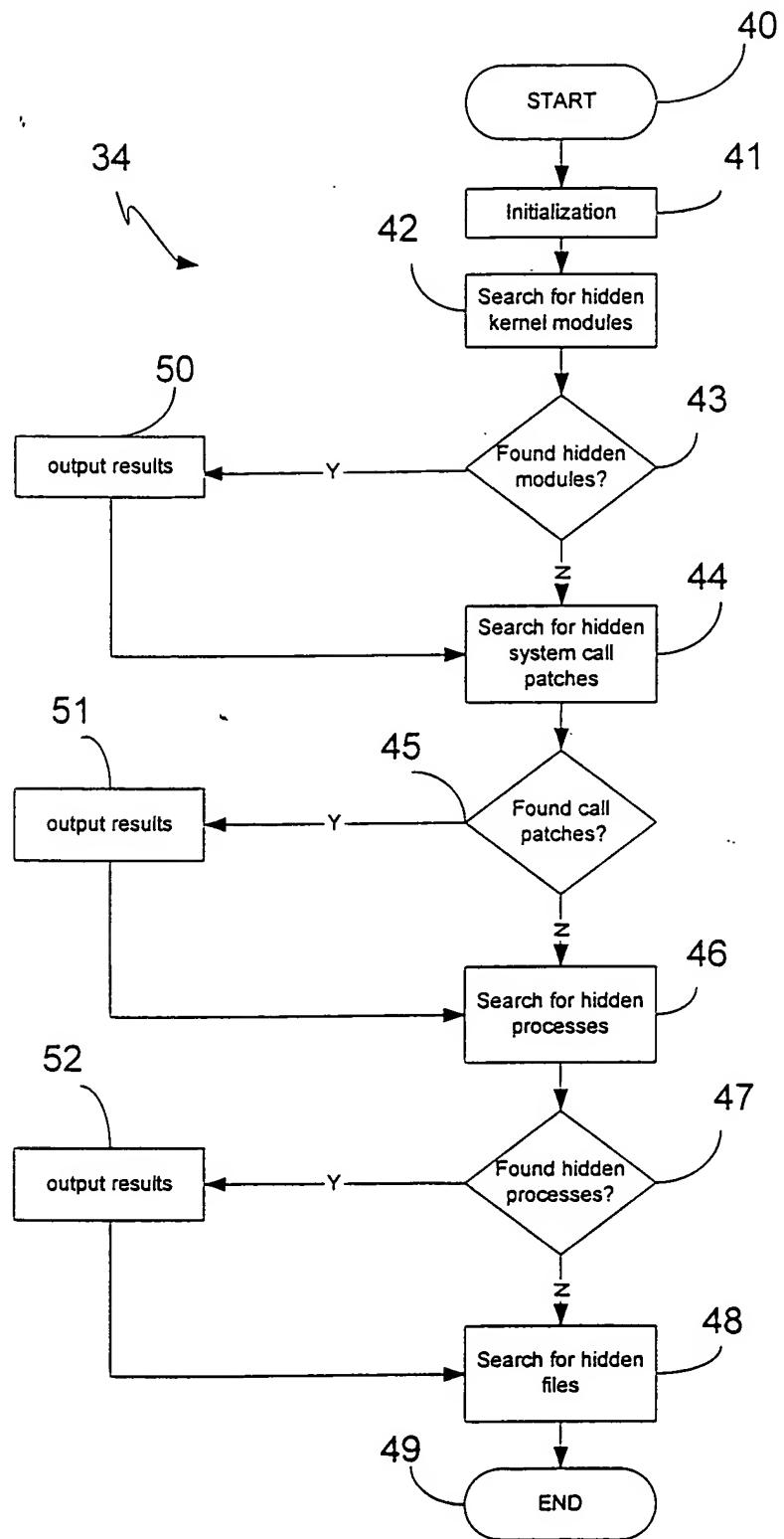
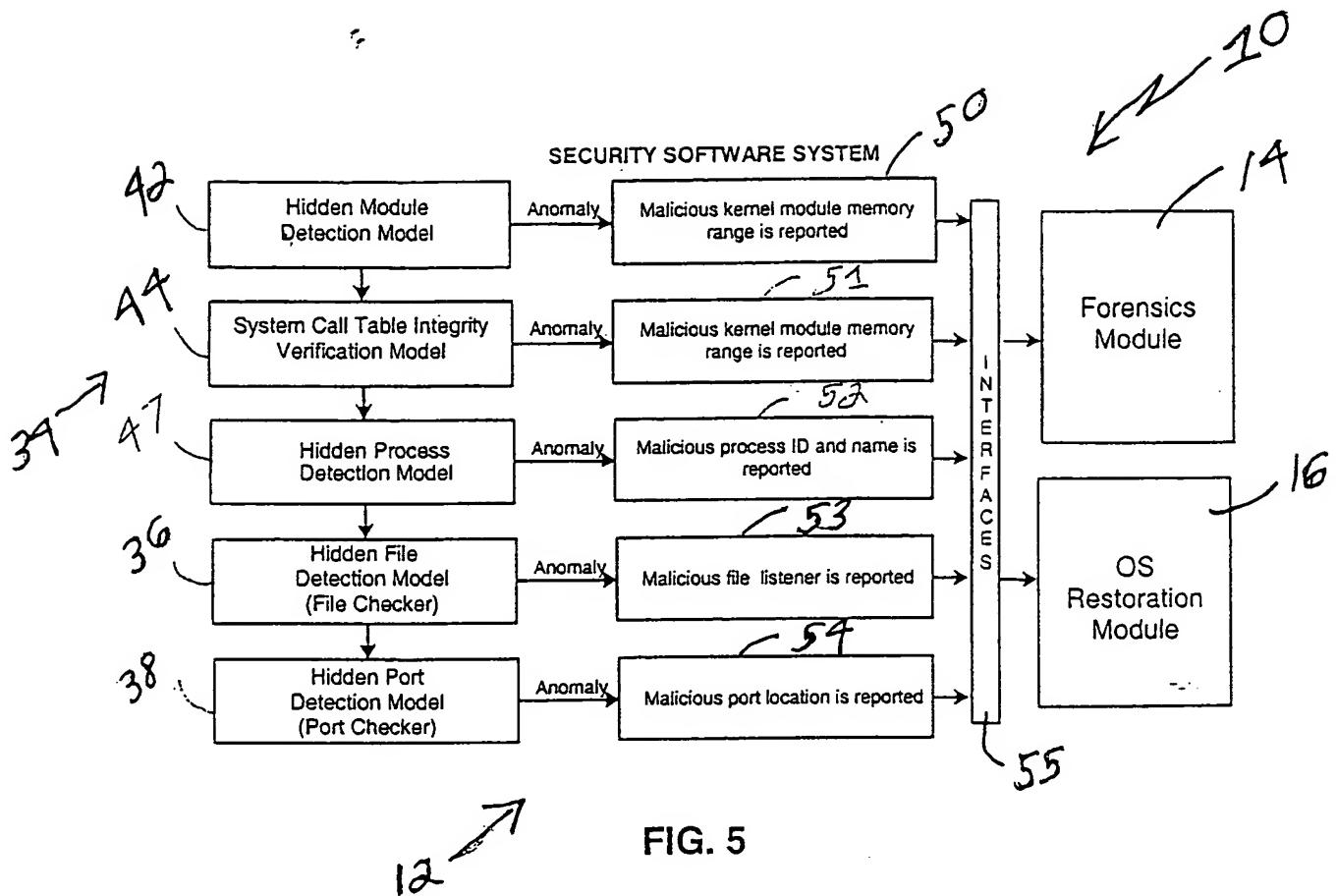


FIG. 4



KERNEL MODULE HIDING
Module list before removal

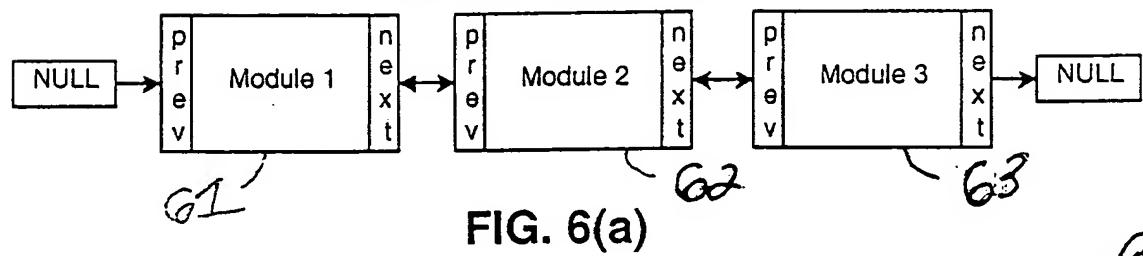


FIG. 6(a)

Module list after hacker technique for removal

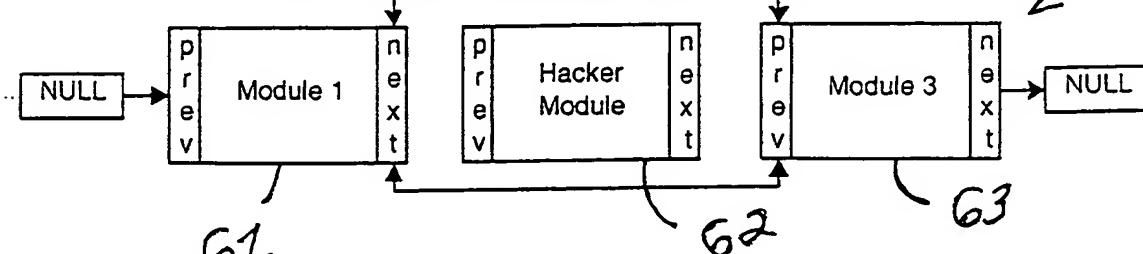


FIG. 6(b)

HIDDEN KERNEL MODULE DISCOVERY MODEL

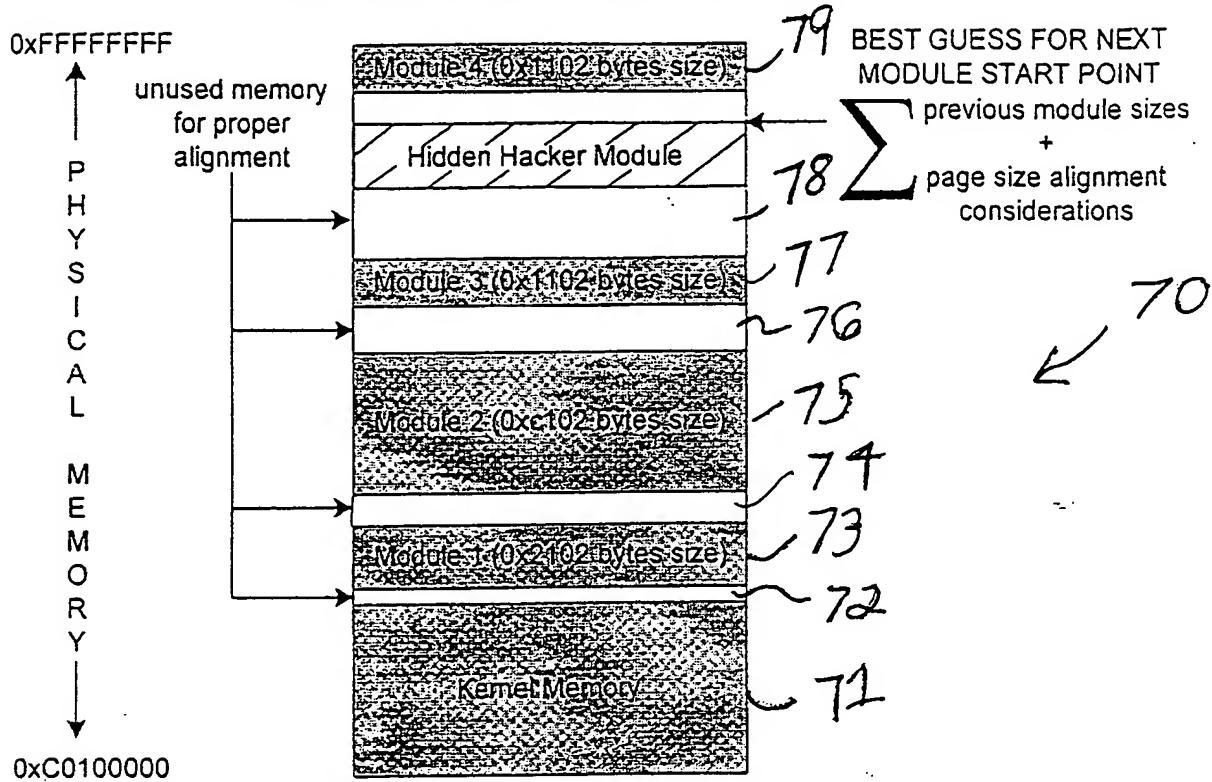


FIG. 7

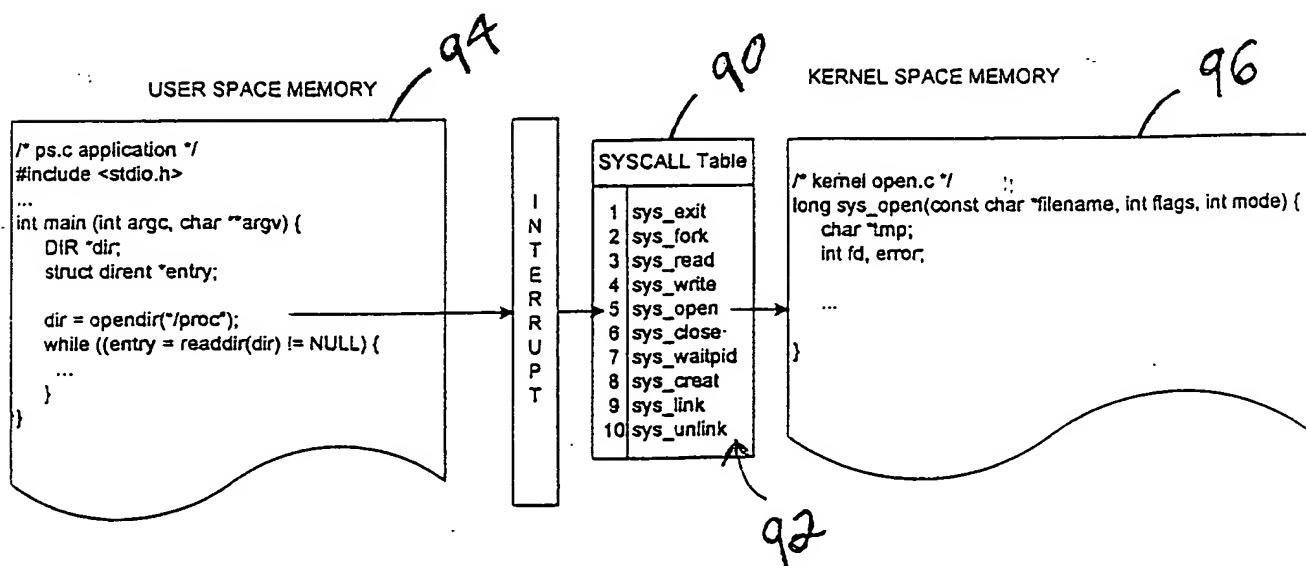


FIG. 9

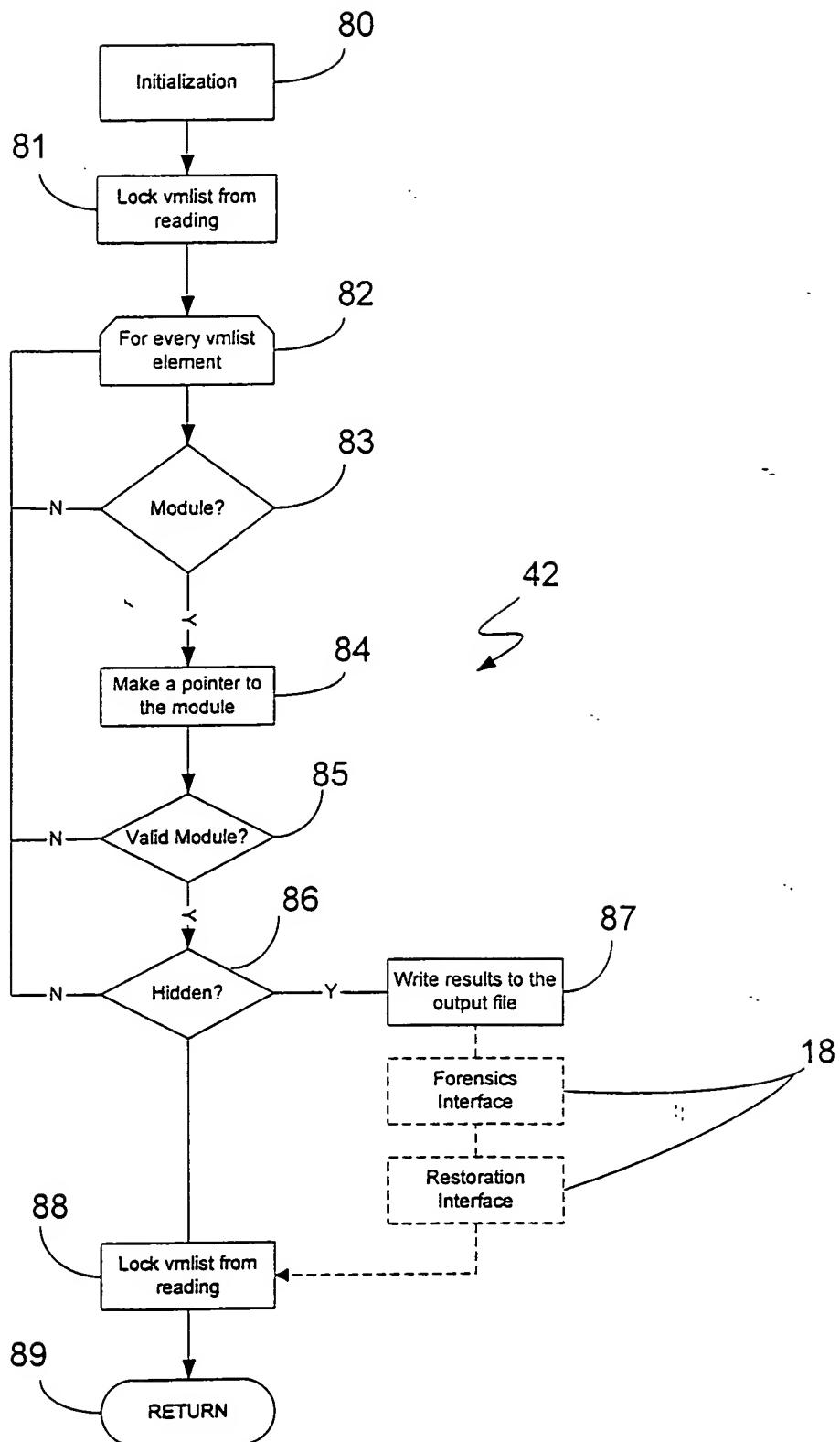


FIG. 8

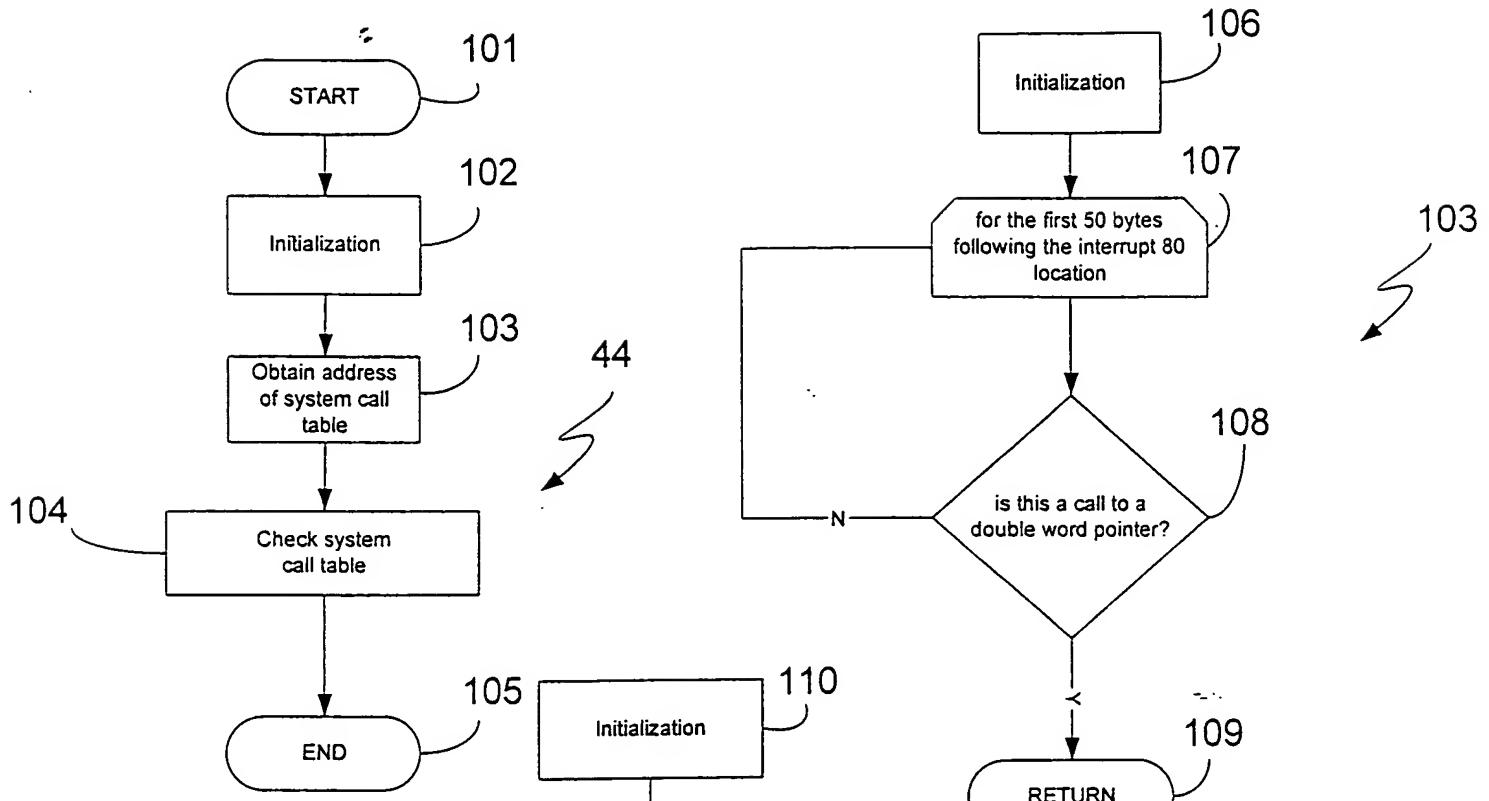


FIG. 10 (a)

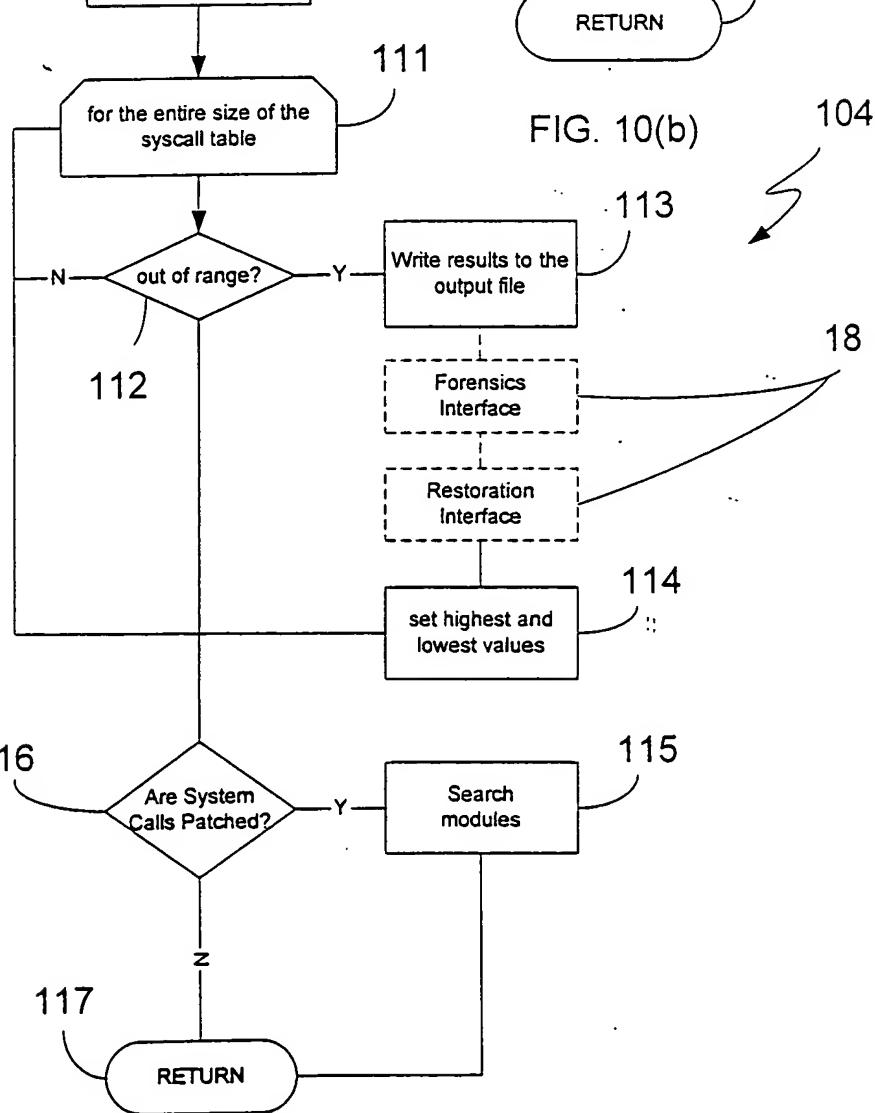


FIG. 10(c)

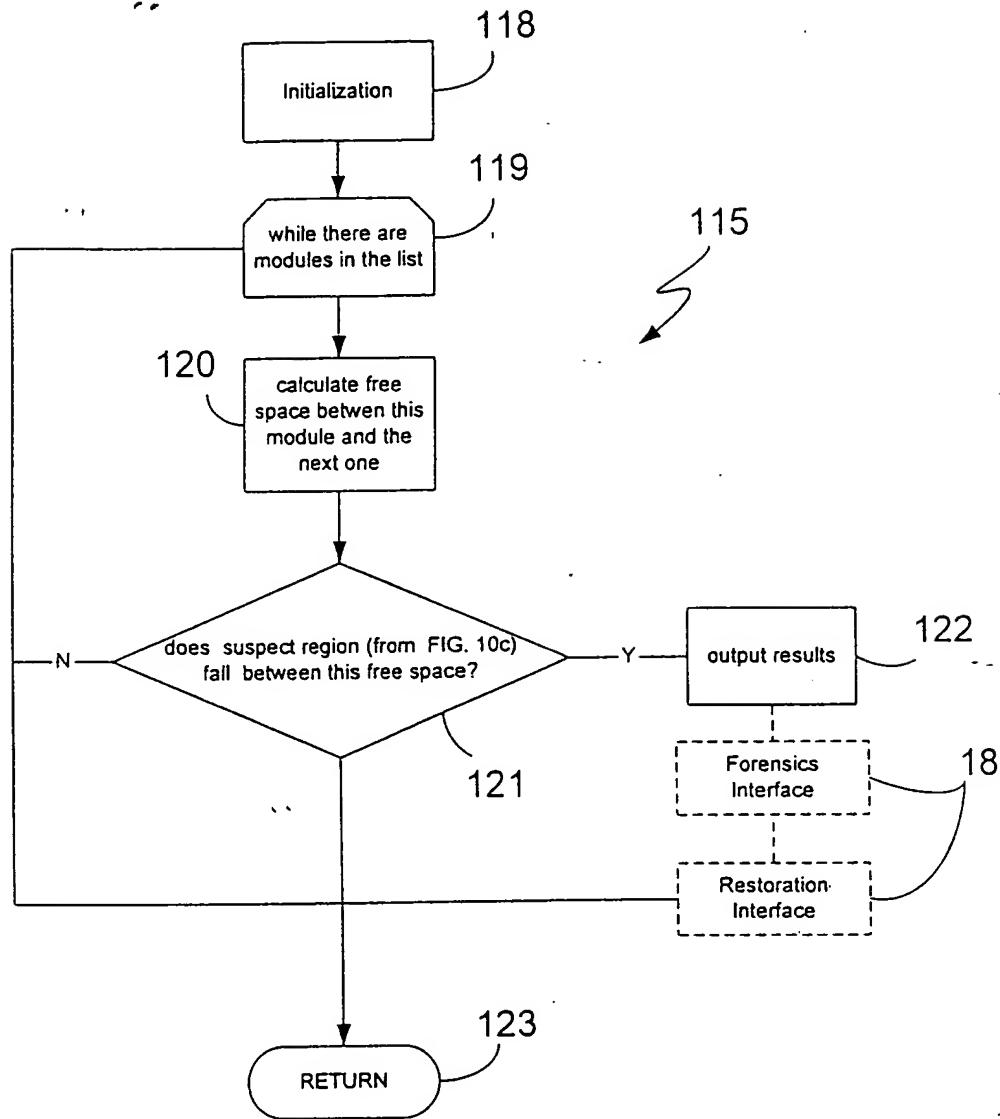


FIG. 10(d)

IDENTIFIED SYSCALL ANOMALIES CAUSE BY ADORE v0.42

syscall[2]	fork	FAILED	0xf8aca650
syscall[4]	write	FAILED	0xf8aca7e8
syscall[5]	open	FAILED	0xf8acb184
syscall[6]	close	FAILED	0xf8aca898
syscall[18]	oldstat	FAILED	0xf8acabef
syscall[37]	kill	FAILED	0xf8aca710
syscall[39]	mkdir	FAILED	0xf8aca9a0
syscall[84]	oldlstat	FAILED	0xf8acacd0
syscall[106]	stat	FAILED	0xf8acacd0
syscall[107]	lstat	FAILED	0xf8aca94
syscall[120]	clone	FAILED	0xf8aca6b0
syscall[141]	getdents	FAILED	0xf8aca368
syscall[195]	stat64	FAILED	0xf8acaf80
syscall[196]	lstat64	FAILED	0xf8acb080
syscall[220]	getdents64	FAILED	0xf8aca4dc

125
Highest

```

analyze_memory(highest, lowest) {
    if the range falls between two
    valid kernel modules then flag
    the entire memory range in
    between the two as a malicious
    kernel module.
}

```

127
Lowest

FIG. 11

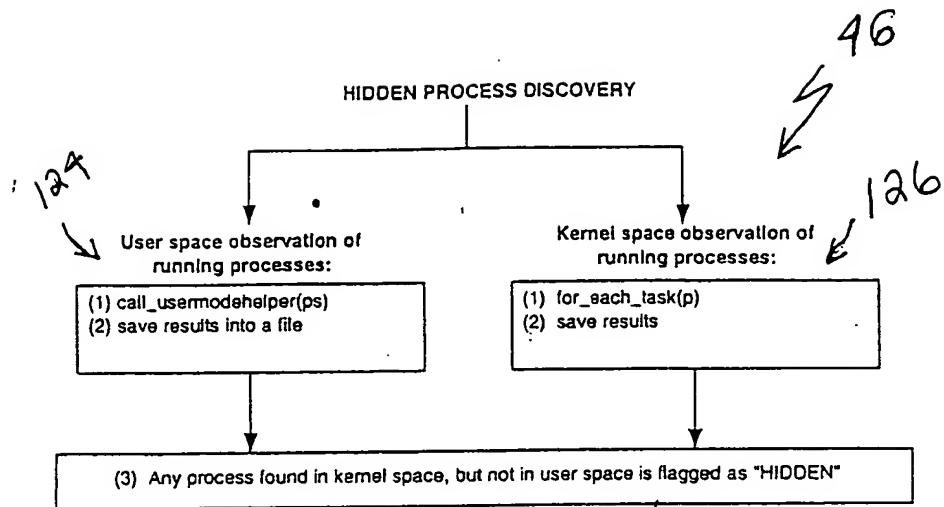


FIG. 12

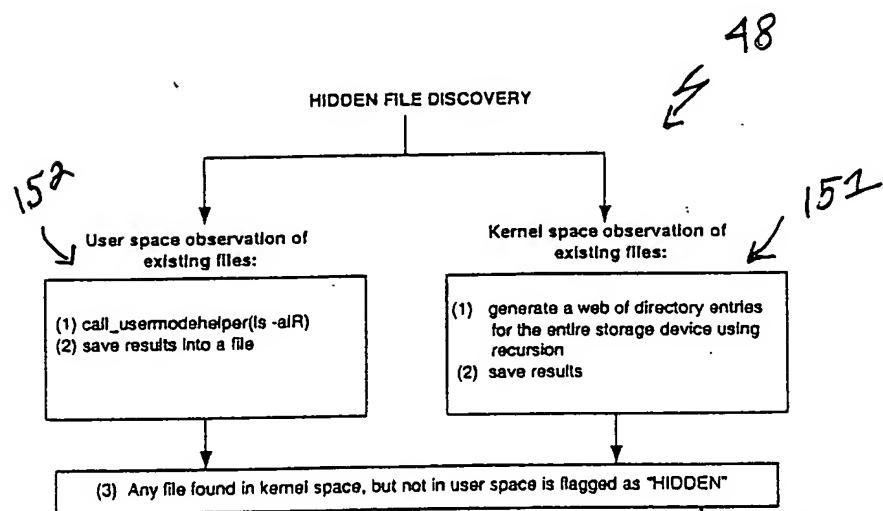


FIG. 15

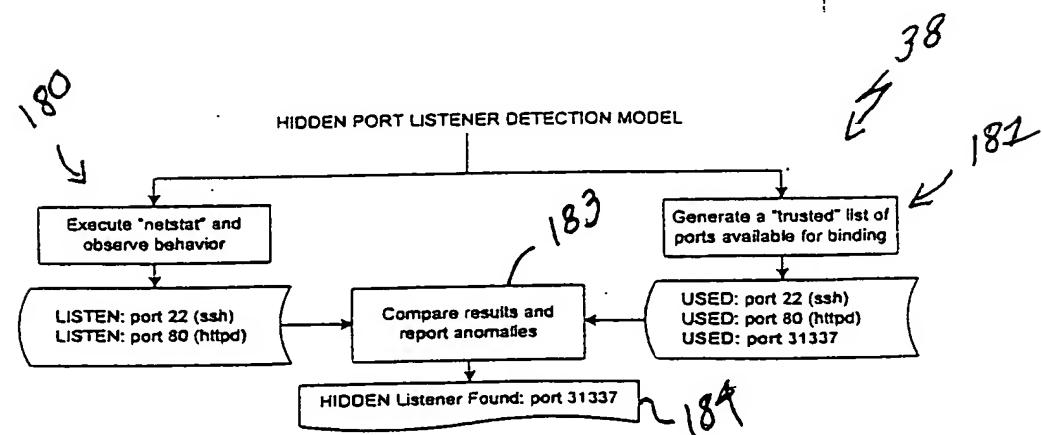


FIG. 18

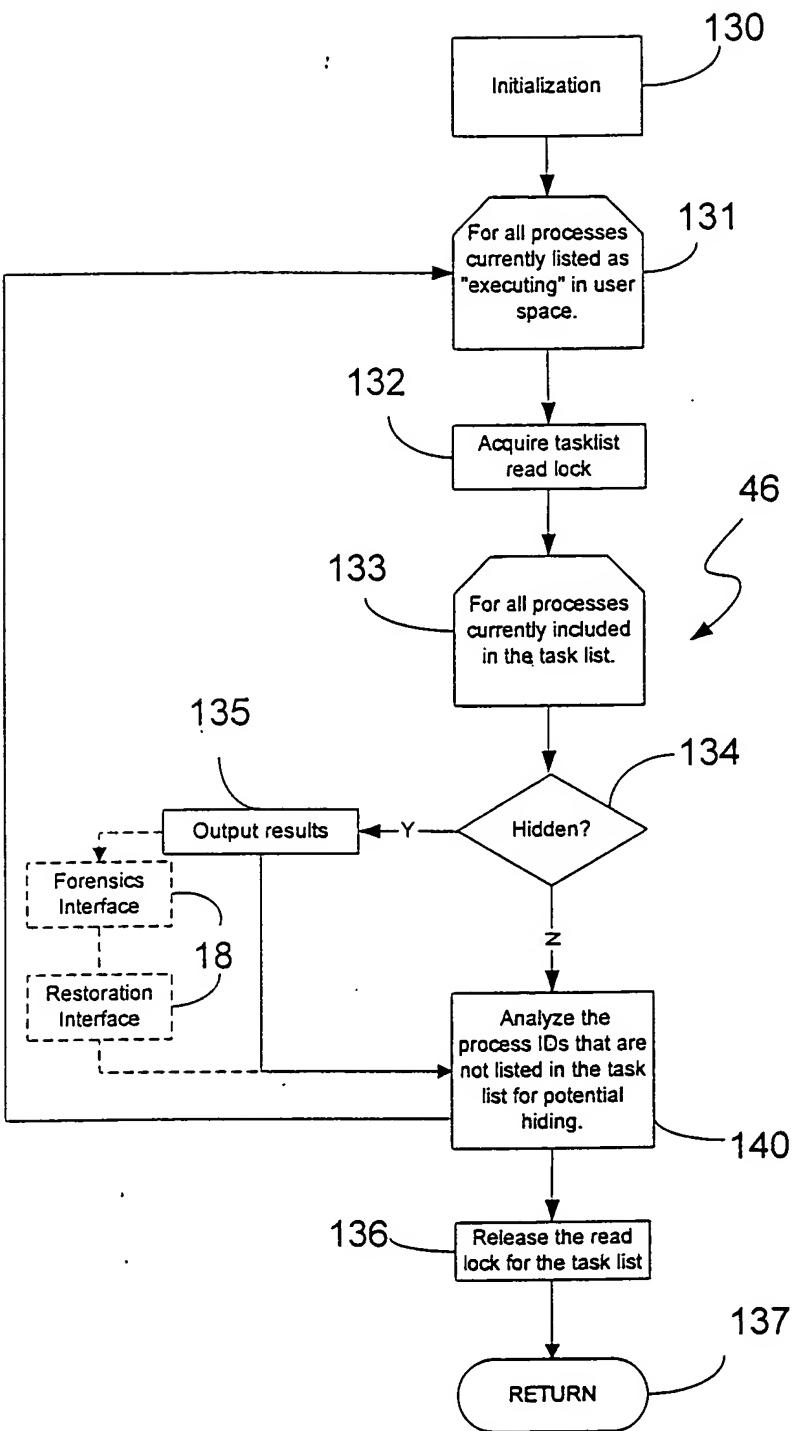


FIG. 13

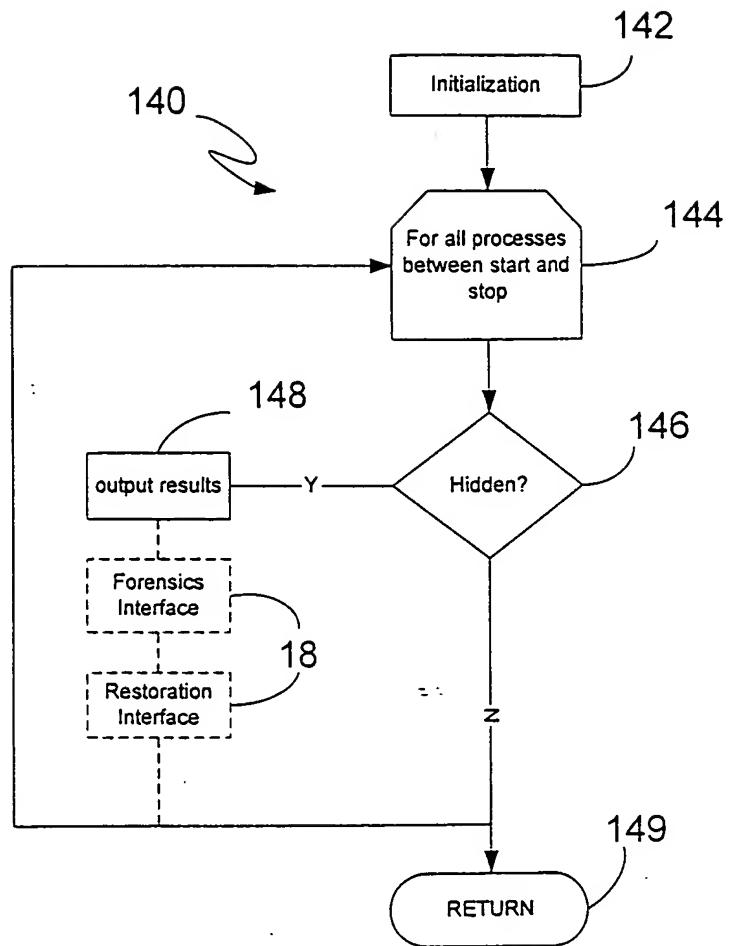


FIG. 14

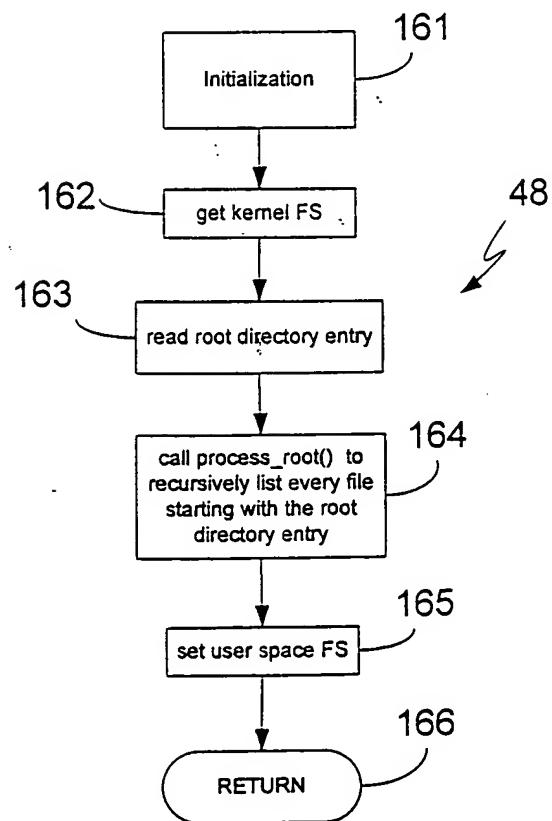


FIG. 16

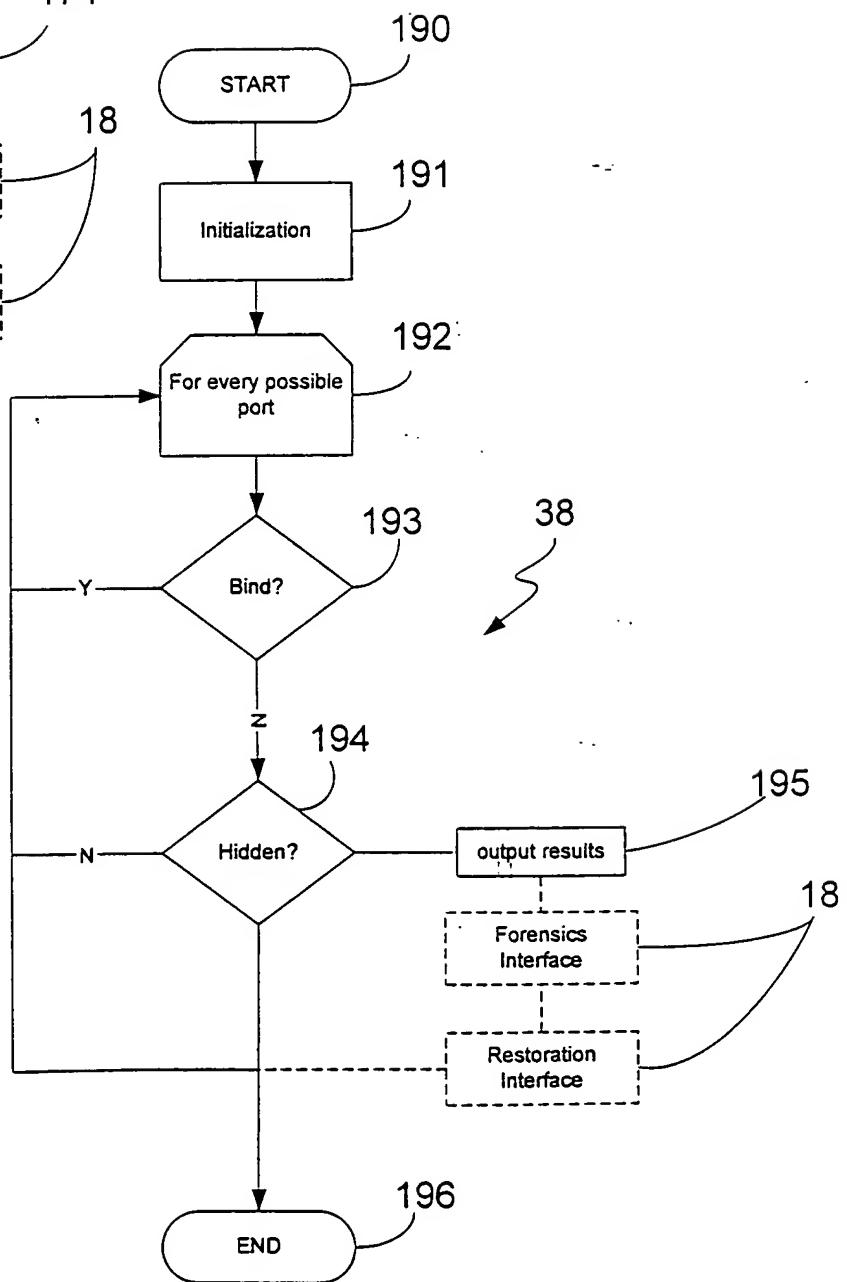
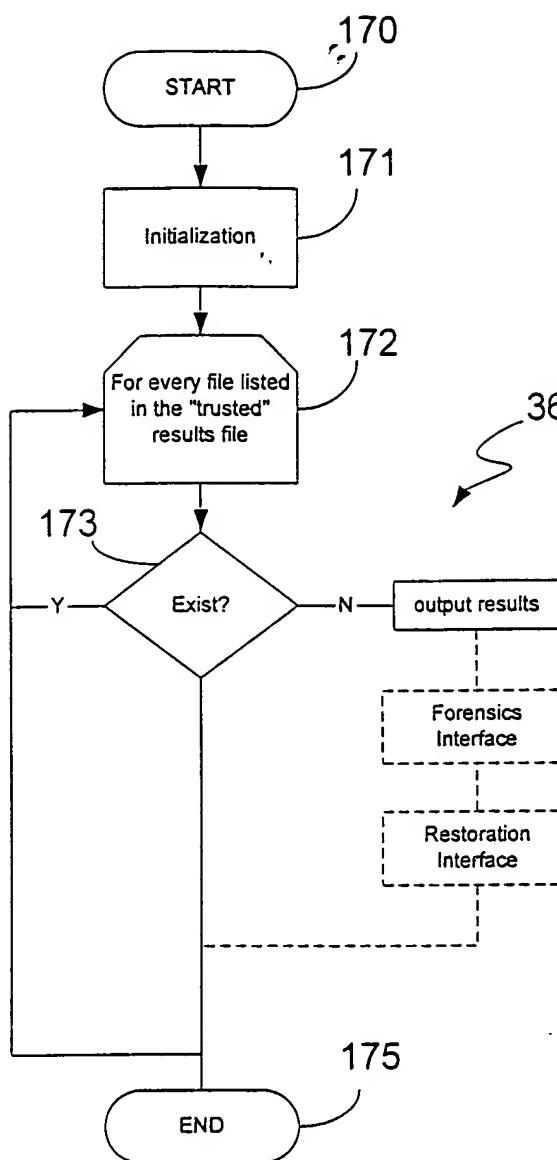


Fig. 17

FIG. 19

Script started on Sat Aug 9 15:42:00 2003
 [root@localhost interrogator]# ./interrogator
 Where would you like the results stored? [/tmp/interrogator/]
 Check for hidden processes? [Y]
 Check for hidden TCP port listeners? [Y]
 Check for system call patching? [Y]
 Check for hidden kernel modules? [Y]
 Check for hidden files? (may take > 15 minutes) [N] Y
 Running the interrogator_ this may take a minute
 Results are located at /tmp/interrogator/summary
 View results now? [Y]

-----{ SUMMARY }-----
 NO hidden modules were found.
 NO system call table modifications were found.
 NO hidden processes were found.
 WARNING: File size is 60133 (should be 58885): /var/log/sa/sa09
 WARNING: File size is 1010871 (should be 1010003): /var/log/cron
 WARNING: File size is 597200 (should be 597264): /var/log/maillog
 NO hidden files were found.
 NO hidden TCP port listeners were found.
 [root@localhost interrogator]# exit
 Script done on Sat Aug 9 16:01:52 2003

208
 209
 FIG. 20(a)

207
 [root@localhost interrogator]# ./interrogator
 Where would you like the results stored? [/tmp/interrogator/]
 Check for hidden processes? [Y]
 Check for hidden TCP port listeners? [Y]
 Check for system call patching? [Y]
 Check for hidden kernel modules? [Y]
 Check for hidden files? (may take > 15 minutes) [N] Y
 Running the interrogator_ this may take a minute
 Results are located at /tmp/interrogator/summary
 View results now? [Y]

-----{ SUMMARY }-----
 NO hidden modules were found.
 NO system call table modifications were found.
 WARNING: process id 13745 hidden or just exited (tb)
 Launch Path: /root/code/interrogator/de.rojansans/tb
 FOUND: 1 Hidden process listing
 HIDDEN File found: /tmp/hideme
 WARNING: File size is 62629 (should be 61381): /var/log/sa/sa09
 WARNING: File size is 1013693 (should be 1012816): /var/log/cron
 WARNING: File size is 599450 (should be 599012): /var/log/maillog
 HIDDEN TCP Port Listener found: port 2222
 [root@localhost interrogator]# exit

207
 FIG. 20(b)

```

[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-----[ SUMMARY ]-----
WARNING suspect module found: f8a0f000 8000 bytes (adore)
Image stored at /tmp/interrogator/adore.o
204
 $\swarrow$ 
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2] FAILED 0xf8a0f650 fork
syscall[4] FAILED 0xf8a0f7e8 write
syscall[5] FAILED 0xf8a10184 open
syscall[6] FAILED 0xf8a0f898 close
syscall[18] FAILED 0xf8a0fbe4 oldstat
syscall[37] FAILED 0xf8a0f710 kill
syscall[39] FAILED 0xf8a0f9a0 mkdir
syscall[84] FAILED 0xf8a0fc0 oldlstat
syscall[106] FAILED 0xf8a0fd8c stat
syscall[107] FAILED 0xf8a0fe94 lstat
syscall[120] FAILED 0xf8a0ff60 clone
syscall[141] FAILED 0xf8a0f368 getdents
syscall[195] FAILED 0xf8a0ff80 stat64
syscall[196] FAILED 0xf8a10080 lstat64
syscall[220] FAILED 0xf8a0f4dc getdents64
Suspect module located (0xf89db6d8 - 0xf8a12000)
FOUND 15 Modified syscall table functions

WARNING: Found process id 836 removed from the task_queue.
Launch Path: /root/code/interrogator/demo/trojans/test
WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 2 Hidden process listings

HIDDEN File found: /tmp/hidame
WARNING: File size is 2336990 (should be 2335392): /var/log/messages

HIDDEN TCP Port Listener found: port 111
HIDDEN TCP Port Listener found: port 139
HIDDEN TCP Port Listener found: port 2222
HIDDEN TCP Port Listener found: port 6000
HIDDEN TCP Port Listener found: port 32768
HIDDEN TCP Port Listener found: port 32769

[root@localhost interrogator]# exit

```

FIG. 20(c)

```

[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-----[ SUMMARY ]-----
WARNING suspect module found: f8a10000 184700 bytes (hamegrown)
206
 $\swarrow$ 
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[3] FAILED 0xf8a11494 read
syscall[5] FAILED 0xf8a11020 open
syscall[11] FAILED 0xf8a10ebc execve
syscall[13] FAILED 0xf8a118a0 time
syscall[78] FAILED 0xf8a1183c gettimeofday
syscall[141] FAILED 0xf8a11544 getdents
syscall[220] FAILED 0xf8a116c0 getdents64
Suspect module located (0xf89db6d8 - 0xf8a3f000)
FOUND 7 Modified syscall table functions

WARNING: process id 1584 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hidame
WARNING: File size is 1021523 (should be 1020648): /var/log/cron
WARNING: File size is 603820 (should be 603384): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit

```

FIG. 20(d)